

UNITED STATES DISTRICT COURT

for the
District of Nebraska

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

RED APPLE IPHONE XR
IMEI # 357349091122697

Case No. 8:20MJ467

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the _____ District of _____ Nebraska _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

21:841, 846

Conspiracy to distribute and possess with intent to distribute controlled substance

The application is based on these facts:

See affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature


☐ Sworn to before me and signed in my presence.

DEA Task Force Officer Kevin Finn

Printed name and title

☒ Sworn to before me by telephone or other reliable electronic means.

Date: 10-14-20


Judge's signature

City and state: Omaha, Nebraska

Susan M. Bazis, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

IN THE MATTER OF THE SEARCH OF
THE FOLLOWING DEVICE WHICH IS
CURRENTLY LOCATED AT THE NSP
OMAHA HEADQUARTERS LOCATED AT
4411 S. 108th ST., OMAHA, NE

Case No. 8:20MJ467

RED APPLE IPHONE XR
IMEI # 357349091122697

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Task Force Officer. Kevin Finn, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of electronic devices which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Nebraska State Patrol Investigator assigned as a Task Force Officer (TFO) with the Drug Enforcement Administration (DEA) and have been so employed since June 2018. I have been a sworn officer of the Nebraska State Patrol (NSP) since 2008. I am currently assigned to the DEA Omaha Division Office, charged with investigating drug trafficking and money laundering violations under Titles 18 and 21 of the United States Code. Your affiant has a Bachelor's Degree in Criminal Justice. Your affiant attended basic training at the Nebraska

State Patrol training academy and received over nine hundred hours of training related to all aspects of law enforcement. Your affiant has attended regular, annual in-service training related to all aspects of law enforcement. Your affiant has been assigned to the Narcotics Investigation Division since July 1, 2015. Your affiant has received over 200 hours of training from the Nebraska State Patrol, DEA, Black Asphalt, FBI, NADDI, Midwest Counter Drug Training Center (MCTC) and International Narcotics Interdiction Association (INIA) in the identification and recognition of illegal drugs, including but not limited to Marijuana, THC oils and wax, Cocaine, Methamphetamine, Fentanyl, Heroin and other controlled substances. Your affiant has been involved, as the primary case officer or a supporting officer, in numerous investigations related to the distribution of controlled substances.

3. I am familiar with the facts and circumstances of this investigation through personal participation and from discussions with agents and officers involved in the investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. This affidavit is submitted in support of a search warrant for the following device which is in the custody of the Nebraska State Patrol, in Omaha, Nebraska:

- a. One red Apple iPhone XR, IMEI #357349091122697, Unknown Model, hereinafter referred to as **DEVICE 1**;

5. The applied-for warrant would authorize the forensic examination of the device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. The United States, including the Drug Enforcement Administration, is conducting a criminal investigation of Rebecca ROMERO DOB: 08/11/90 and any unidentified co-conspirators regarding possible violations of Title 21 United States Code, Sections 841 and 846.

7. Analysis of intelligence collected on ROMERO revealed an operators licenses out of Wisconsin, with an address of 5782 Tudor Dr. Fitchburg, WI, and a surrendered license out of Nebraska with an address of 1315 W. 6th St. in North Platte. Both operators' licenses bearing a date of birth of 08/11/90.

8. On September 19, 2020, staff of the Hartig Pharmacy located in Dubuque, Iowa alerted investigators that conspirators known to this investigation were attempting to fill fraudulent prescriptions. The Dubuque Police Department was notified, at which point contact was made detaining Cameron ALEXANDER, Malik BRAGG, and Rebeca ROMERO. A search conducted by Dubuque Police lead to the seizure of a .45 caliber Springfield XD (SN: 459652), three empty bottle of Promethazine with Codeine, a full bottle of Promethazine with Codeine, numerous fraudulent Rx scripts and approximately sixteen grams of marijuana.

9. Romero was arrested and interviewed by Dubuque Iowa Police Officer Blum, **DEVICE 1** was located in her possession, according to reports from Blum, Romero gave a pass code of 926411 for **DEVICE 1**. **DEVICE 1** was seized by DPD and turned over to Nebraska State Patrol for storage and analysis.

10. On September 21, 2020, investigators conducted an interview of Cameron ALEXANDER who stated that he had been traveling from Iowa City, Iowa prior to being detained by law enforcement in Dubuque, Iowa. Analysis of Precision Location Information data indicates that the telephone associated to the number (312)343-0863, found in possession

of ALEXANDER, was tracked from Madison, Wisconsin to Dubuque, Iowa and had never gone to Iowa City, contradicting statements made by ALEXANDER. Investigators believe Alexander lives with and is in a relationship with ROMERO and they have a child together. Romero and BRAGG refused an interview.

11. A review of call detail records for **DEVICE 1** between December 27, 2019 and September 7, 2020, show 3,329 contacts with 312-343-0863 (Cameron Alexander), 90 contacts with 608-216-8527 (Malik Bragg), 80 contacts with 308-289-6933 Julius Reed and 1 contact with 818-319-2561 (Dr. Raphael Malikian). Investigators are aware these individuals have been engaging in a conspiracy to obtain controlled substances through various pharmacies across the Midwest by creating fraudulent patient profiles through Dr. Raphael Malikian.

12. Based on the above facts, agents believe that Rebecca ROMERO is obtaining Pharmaceutical controlled substance illegally. Furthermore, based on details of this investigation TFO Finn knows that Rebecca ROMERO utilizes **DEVICE 1** during the course of obtaining pharmaceutical controlled substances, therefore TFO Finn believes that **DEVICE 1** will assist agents in identifying the method in which Malik BRAGG is obtaining the controlled substances.

13. **DEVICE 1** is currently in the lawful possession of the Nebraska State Patrol, in Omaha, Nebraska. While the Nebraska State Patrol, in Omaha, Nebraska might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

TECHNICAL TERMS

14. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include

various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna

can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- g. Memory Card: A memory card is utilized in many different types of devices (such as cellular phones, PDAs, GPS Units etc). These memory cards can contain any type of digital data to include pictures, keystroke information, telephone numbers,

contact lists, calendars etc. These items in and of themselves are portable and may be used in multiple devices.

15. Based on my training and experience I am aware that the Device requested to be searched has the capability that allows it to serve as a wireless telephone and has the capability to include but not limited to, digital camera, portable media player, GPS navigation device and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

16. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

17. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

18. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Devices consistent with the warrant. The examination may require authorities to employ techniques, including but

not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

19. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

20. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

21. Based upon my experience and training, I know that drug traffickers commonly possess and use digital devices such as cellular telephones in connection with their drug trafficking activities. These devices typically store relevant information concerning their drug activities and drug associates including addresses and telephone numbers, text messages, multi-media messages, the times and dates of incoming and outgoing calls and messages, and electronic files such as photographs, and videos.

22. I know from my training and experience that members of Drug Trafficking Organizations (DTO) commonly communicate with cellular telephones, to include text messaging and multi-media messaging. I also know that members of DTO's commonly store phone numbers for their drug suppliers, co-conspirators and customers in their cell phones. The numbers stored in **DEVICE 1's** phone logs could have significance to ongoing narcotics investigations, as well as possible connections to potential targets in this case.

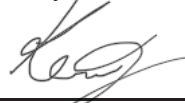
23. In addition, I know from my training and experience that because drug dealing is a very mobile business, it is necessary for persons involved in the drug business to use electronic communication devices such as cellular telephones so that they can conduct their drug business at virtually any time without unnecessary delay. I know that these devices are capable of storing information such as phone numbers and/or coded messages which may lead to the identity of codefendants, coconspirators, and/or sources of supply. Cellular telephones, in addition to being communication devices, are also storage devices for data. Data electronically stored inside cellular telephones include telephone numbers of associates, logs of the date and time that individual calls were made, voice and electronic messages from associates and photographs or videos of the primary user, associates, and co-conspirators. The data inside cellular telephones is evidence of drug trafficking, demonstrates true ownership and control of the telephones, which are often registered to another person, and can be effectively used to corroborate the statements of witnesses.

24. In addition, based on my training and experience, drug traffickers often have photographs or videos in cellular phones, of themselves, their coconspirators and property/assets purchased with drug proceeds. These photographs and videos often contain evidence of drug trafficking and evidence of the use of cash proceeds to make purchases of various assets, such as vehicles or jewelry. Further, these photographs and videos are useful to identify sources of supply, customers, associates, and co-conspirators of the primary user of the telephone as well as vehicles used or owned, places of operation or storage, and other evidence of drug trafficking activities.

25. Based on the foregoing, there is probable cause to believe the data and information electronically stored within the Device such as but not limited to details of past telephone contacts

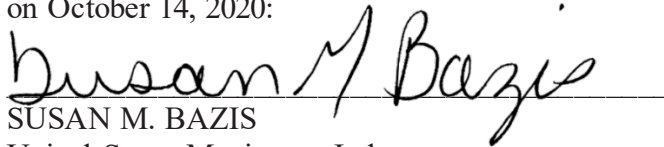
and records of calls made and received, text messages, multi-media messages, voice mails, internet browser history, types, amounts and prices of drugs trafficked, as well as dates, places and amounts of specific transactions, any information related to the sources of drugs (including names, addresses, phone numbers, or any other identifying information), any information related to schedule or travel, including geographic location information, photographs, videos, and audio files, and evidence of user attribution such as logs, phonebooks, and saved usernames and passwords, contain evidence of the commission of the above-listed violations, evidence concerning the fruits of the above described criminal activities, and/or evidence concerning the means of committing a violation of the above-listed statutes. Accordingly, I request authority to allow technicians to search the Device for evidence such as that described above.

Respectfully submitted,



Kevin P. Finn
Task Force Officer

Subscribed and sworn to before me
on October 14, 2020:



SUSAN M. BAZIS
United States Magistrate Judge

ATTACHMENT A

1. This affidavit is submitted in support of a search warrant for the following devices which are in the custody of the Nebraska State Patrol, located at 4411 S. 108th Street, Omaha, Nebraska 68137.

b. One red Apple iPhone XR, IMEI # 357349091122697 hereinafter referred to as
DEVICE 1;

2. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations under Title 21, United States Code, Controlled Substance Act, Title 18, United States Code, Laundering of Monetary Instruments and information pertaining to the user the Device:

- a. Visual depictions of sent and/or received files (including but not limited to still images, videos, films or other recordings) or other computer graphic files;
- b. Electronic copies of log files, to include but not limited to: emails, instant messaging, audio, still images, video recordings, chat logs, social media data, and digital cloud data stored on or about computer hardware. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Any and all hardware/mechanisms used for the receipt or storage of the same, including but not limited to: any computer system and related peripherals, including data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, hard drives, tape drives, disk drives, transistor-binary devices, magnetic media disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, usb storage devices and flash memory storage devices, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, optical readers, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices,

electronic tone generating devices, and related communications devices such as modems, cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

- c. Electronic data contained in cellular phone, including any names, co-conspirators, associates, phone numbers, addresses, contact information, data, text, messages, images, voice memos, voice mail, GPS or specific location information, maps and directions, calendar, photographs, videos, internet sites, internet access, documents, emails and email accounts, social media accounts, cloud storage accounts, or other information, ledgers, contained in the cellular phone internal, external or removable memory or memories, which includes any smart cards, SIM cards or flash cards;
- d. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code;
- e. Documents, records, emails, and internet history (in documentary or electronic form) whether transmitted or received;
- f. Records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, including but not limited to social media accounts, cloud storage accounts, and email accounts, as well as any and all records relating to the ownership or use of the computer hardware, digital device and/or digital media account;

- g. Digital documents and records regarding the ownership and/or possession of the searched premises;
- h. During the course of the search, photographs of the searched items may also be taken to record the condition thereof and/or the location of items therein.

UNITED STATES DISTRICT COURT

for the
District of Nebraska

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Case No. 8:20MJ467

RED APPLE IPHONE XR)
IMEI # 357349091122697)
)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer ,

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the _____ District of _____ Nebraska
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before October 28, 2020 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Susan M. Bazis
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 10-14-20 at 4:09 p.m.


Judge's signature

City and state: Omaha, Nebraska

Susan M. Bazis, U.S. Magistrate Judge
Printed name and title

ReturnCase No.:
8:20MJ467

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

1. This affidavit is submitted in support of a search warrant for the following devices which are in the custody of the Nebraska State Patrol, located at 4411 S. 108th Street, Omaha, Nebraska 68137.

b. One red Apple iPhone XR, IMEI # 357349091122697 hereinafter referred to as
DEVICE 1;

2. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations under Title 21, United States Code, Controlled Substance Act, Title 18, United States Code, Laundering of Monetary Instruments and information pertaining to the user the Device:

- a. Visual depictions of sent and/or received files (including but not limited to still images, videos, films or other recordings) or other computer graphic files;
- b. Electronic copies of log files, to include but not limited to: emails, instant messaging, audio, still images, video recordings, chat logs, social media data, and digital cloud data stored on or about computer hardware. Computer hardware, that is, all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Any and all hardware/mechanisms used for the receipt or storage of the same, including but not limited to: any computer system and related peripherals, including data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, hard drives, tape drives, disk drives, transistor-binary devices, magnetic media disks, external hard drives, floppy disk drives and diskettes, routers, computer compact disks, CD-ROMS, DVD, usb storage devices and flash memory storage devices, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, optical readers, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices,

electronic tone generating devices, and related communications devices such as modems, cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

- c. Electronic data contained in cellular phone, including any names, co-conspirators, associates, phone numbers, addresses, contact information, data, text, messages, images, voice memos, voice mail, GPS or specific location information, maps and directions, calendar, photographs, videos, internet sites, internet access, documents, emails and email accounts, social media accounts, cloud storage accounts, or other information, ledgers, contained in the cellular phone internal, external or removable memory or memories, which includes any smart cards, SIM cards or flash cards;
- d. Any and all computer passwords and other data security devices designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code;
- e. Documents, records, emails, and internet history (in documentary or electronic form) whether transmitted or received;
- f. Records, documents, invoices, notes and materials that pertain to accounts with any Internet Service Provider, including but not limited to social media accounts, cloud storage accounts, and email accounts, as well as any and all records relating to the ownership or use of the computer hardware, digital device and/or digital media account;

- g. Digital documents and records regarding the ownership and/or possession of the searched premises;
- h. During the course of the search, photographs of the searched items may also be taken to record the condition thereof and/or the location of items therein.